RATIONAL POINTS ON ELLIPTIC CURVES

GRAHAM EVEREST, JONATHAN REYNOLDS AND SHAUN STEVENS

February 2, 2008

Abstract. We consider the structure of rational points on elliptic curves in Weierstrass form. Let $x(P) = A_P/B_P^2$ denote the x-coordinate of the rational point P then we consider when B_P can be a prime power. Using Faltings' Theorem we show that for a fixed power greater than 1, there are only finitely many rational points with this property. Where descent via an isogeny is possible we show, with no restrictions on the power, that there are only finitely many rational points with this property, that these points are bounded in number in an explicit fashion, and that they are effectively computable.

Let E denote an elliptic curve given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

with integral coefficients $a_1, \ldots, a_6$. See [1] and [15] for background on elliptic curves. Let $E(\mathbb{Q})$ denote the group of rational points on E. For an element $P \in E(\mathbb{Q})$, the shape of the defining equation (1) requires that P be in the form

$$P = \left(\frac{A_P}{B_P^2}, \frac{C_P}{B_P^3}\right) \tag{2}$$

where A_P, B_P, C_P are integers with no common factor. In this paper we are concerned with the equation

$$B_P = p^f \tag{3}$$

where p denotes a prime and $f \geq 1$ denotes an integer. All of the methods extend to the equation $B_P = bp^f$, where b is fixed, with trivial adjustments. Gunther Cornelissen once remarked to the first author that the equation (3) has only finitely many solutions when $f = 2$, by re-arranging the equation and invoking Faltings' Theorem.

1991 *Mathematics Subject Classification.* 11G05, 11A41.

Key words and phrases. Siegel's Theorem, elliptic curve, prime.

The authors thank Gunther Cornelissen and Jan-Hendrik Evertse for helpful comments.

Theorem 0.1. *Let E denote an elliptic curve in Weierstrass form (1). For any fixed $f > 1$, there are only finitely many P for which equation (3) has a solution, with p denoting any integer.*

The proof is based upon one of Siegel's proofs of his theorem about S-integral points, and uses Faltings' Theorem at a critical stage. In his thesis [13], the second author gives a generalization of Theorem 0.1 to number fields.

Where descent via an isogeny is possible, Theorem 0.1 can be strengthened. If G denotes a subset of $E(\mathbb{Q})$, let r_G denote the rank of the subgroup of $E(\mathbb{Q})$ generated by G. Given an elliptic curve E, let Δ_E denote the discriminant of E. Finally, let $\omega(N)$ denotes the number of distinct prime factors of the integer N.

Theorem 0.2. *Let E denote an elliptic curve and let G denote a given subset of $E(\mathbb{Q})$. Assume G lies in the image of a non-trivial isogeny from a subset G' of $E'(\mathbb{Q})$, for an elliptic curve E'. There are only finitely many P for which equation (3) has a solution, where p denotes any prime, and f denotes any integer $f \geq 1$. The exceptional points can be computed effectively, and they are at most*

$$\theta^{(r_G+1)\omega(\Delta_E)}, \tag{4}$$

in number, where $\theta > 1$ is a uniform constant which can be presented explicitly.

Note the crucial distinctions: in Theorem 0.2 both p and f are allowed to vary whereas in Theorem 0.1 the exponent f is fixed beforehand. Also Theorem 0.2 deals with the case $f \geq 1$ whereas Theorem 0.1 assumes $f > 1$. The effectiveness statement assumes the *givenness* of the set G; typically G will consist of the linear span of a finite set of points.

The effective and explicit nature of Theorem 0.2 renders this a much stronger outcome. The effectiveness statement is possibly of more moral than practical worth. The tools used include elliptic transcendence theory which, on the face of it, exhibits a large bound for the height of the exceptional points. In practice, the bounds are usually much smaller. Indeed, infinite families can be constructed with very small exceptional sets.

Example 0.3 ([13])**.** For every integer $T > 1$ consider the elliptic curve

$$y^2 = (x+1)(x-T^2)(x-T^4)$$

together with the rank-1 subgroup generated by the point $P = (0, T^3)$. For all $T > 1$ and all $n > 2$ the denominator of $x(nP)$ is divisible by at least two distinct primes. More will be said about this example at the conclusion of Section 2.3.

Our third theorem concerns curves in homogeneous form. Suppose E denotes an elliptic curve defined by an equation

$$u^3 + v^3 = D, \tag{5}$$

for some non-zero $D \in \mathbb{Q}$. Let P denote a non-torsion $\mathbb{Q}$-rational point. Write, in lowest terms

$$P = \left(\frac{A_P}{B_P}, \frac{C_P}{B_P} \right). \tag{6}$$

Theorem 0.4. *Suppose E denotes an elliptic curve defined by an equation (5) for some non-zero cube-free $D \in \mathbb{Q}$. Let P denote a non-torsion point in $E(\mathbb{Q})$. With P as in (6), the integers B_P are prime powers for at most $\mu^{\omega(D)}$ points P, where $\mu > 1$ is a uniform constant which can be presented explicitly.*

0.1. **Prime Denominators.**

The equation $B_P = p$ (in other words $f = 1$) occupies something of a middle ground between Theorems 0.1 and 0.2. The possibilities do seem to be more subtle. In [2], [4], [7] and [8], this apparently more difficult question has been considered. In [7] and [8] we argued that, for rank-1 subgroups G (in other words, multiples of a single point) only finitely many points $P \in G$ should yield prime values B_P. In certain cases, we could prove this and we conjectured that, for a rank-1 subgroup G, the number of rational points $P \in G$ as in (2), with B_P a prime is uniformly bounded if the defining equation (1) is in minimal form. Many calculations suggest that for an elliptic curve in minimal form, a little over 30 prime values B_P seems to be the limit. The following example may well provide the limiting case. It is taken from Elkies' table of small height points in [5]. Note that the curves in Elkies' table are not presented in minimal form; the example following is the second on the list, with the equation rendered in minimal form. The point shown has the second smallest known height amongst all rational points on elliptic curves.

Example 0.5. Let P denote the point $P = (-386, -3767)$ on the elliptic curve

$$y^2 + xy = x^3 - 141875x + 13893057.$$

The values $x(nP)$ have prime square denominators for 31 values of n, ending with (apparently) $n = 613$. The first example on Elkies' list yields (apparently) 30 such primes. These computations were performed using PARI-GP.

In a short subsection (§2.3) we will give an outline of a proof of uniformity assuming an unproven (yet generally believed conjecture) as well as an improvement to known results in elliptic transcendence theory.

On the other hand, in [6], many examples of rank-2 curves were considered where, apparently, there are infinitely many rational points P with B_P prime.

Example 0.6. The curve

$$y^2 = x^3 - 28x + 52$$

has rank 2, with generators $P_1 = (-2, 10)$ and $P_2 = (-4, 10)$. In [6] we considered the possibility that asymptotically $\rho \log T$ values

$$x(n_1P_1 + n_2P_2) \text{ with } \max\{|n_1|, |n_2|\} < T$$

possess a prime square denominator, where $\rho > 0$ is a constant depending upon E. The table in [14], constructed by Peter Rogers, exhibits many more rank-2 curves which are thought to yield infinitely many rational points P as in (2) with B_P a prime.

Theorem 0.2 allows many examples which yield only finitely many primes to be constructed, when a descent is possible.

Example 0.7. The curve

$$y^2 = x^3 - 6400x + 192000$$

has rank 2, with independent points $P_1 = (65, 225)$ and $P_2 = (56, 96)$. Theorem 0.2 guarantees there are finitely many prime square denominators amongst the points $n_1P_1 + n_2P_2$ because the points shown are the images of the points $(0, 100)$ and $(6, 104)$ under a 2-isogeny from the curve

$$y^2 = x^3 + 100x + 10000.$$

In Section 1 we give a proof of Theorem 0.1: since it relies on Faltings' Theorem, it is not effective. Following this, we prove Theorem 0.2; the effectiveness statement uses local heights and elliptic transcendence theory whilst the explicit bound for the exceptional points relies upon a strong version of Siegel's Theorem [11], [16]. The final section proves Theorem 0.4, using a strong form of Thue's Theorem to rid us of the dependence upon the rank.

1. Proof of Theorem 0.1

Let K be a finite field extension of $\mathbb{Q}$. The valuations on K, written M_K, consist of the usual archimedean absolute values together with the non-archimedean, $\wp$-adic valuations, one for each prime ideal $\wp$ of K. Write K_v for the completion of K with respect to v. Let $S \subset M_K$ denote a finite set of valuations containing the archimedean valuations. The ring O_S of S-integers is given by

$$O_S = \{x \in K : \nu(x) \geq 0 \text{ for all } \nu \in M_K, \nu \notin S\}$$

and the unit group O_S^* of O_S is given by

$$O_S^* = \{x \in K : \nu(x) = 0 \text{ for all } \nu \in M_K, \nu \notin S\}.$$

Completing the square in (1), it is sufficient to consider an equation

$$y^2 = x^3 + a_2x^2 + a_4x + a_6 \tag{7}$$

where $x^3 + a_2x^2 + a_4x + a_6 \in \mathbb{Q}[x]$ has distinct zeros $\alpha_1, \alpha_2, \alpha_3$ in some finite extension K of $\mathbb{Q}$. Of course we might have introduced powers of 2 into the denominators in (7); we will see that this does not matter.

Let S be a sufficiently large (finite) subset of M_K so that O_S is a principal ideal domainand $2, \alpha_i - \alpha_j \in O_S^*$ for all $i \neq j$. Now let L/K be the extension of K obtained by adjoining to K the square root of every element of O_S^*. Note that L/K is a finite extension, since $O_S^*/(O_S^*)^2$ is finite from Dirichlet's S-unit theorem. Further let $T \subset M_L$ be a finite set containing the places of L lying over elements of S and such that O_T is a principal ideal domain, where, by abuse of notation, O_T denotes the ring of T-integers in L.

Now we turn to the proof of the Theorem. Replacing (x, y) by $(x/q^2, y/q^3)$ in (7), we are searching for solutions in $\mathbb{Q} \cap O_S$ to

$$y^2 = x^3 + a_2q^2x^2 + a_4q^4x + a_6q^6, \qquad \gcd(xy, q) = 1. \tag{8}$$

We will show that, for fixed $f > 1$, there are only finitely many prime powers $q = p^f \in \mathbb{Z}$ for which (8) has a solution. Note that, since f is fixed and T is finite, we may assume that p is large enough so that no valuation of L dividing p lies in T.

Let $x, y \in \mathbb{Q} \cap O_S$ be a solution to (8); then

$$y^2 = (x - q^2\alpha_1)(x - q^2\alpha_2)(x - q^2\alpha_3). \tag{9}$$

Let $\wp$ be a prime ideal of O_S dividing $x - q^2\alpha_i$; then $\wp$ cannot divide q, since $(x, q) = 1$. Hence $\wp$ can divide at most one term $x - q^2\alpha_i$, since if it divides both $x - \alpha_iq^2$ and $x - \alpha_jq^2$ then it divides also $(\alpha_i - \alpha_j)q^2$. From (9) it follows that there are elements $z_i \in O_S$ and units $b_i \in O_S^*$ so that

$$x - \alpha_iq^2 = b_iz_i^2.$$

We have $b_i = \beta_i^2$, for some $\beta_i \in O_T$ so

$$x - \alpha_iq^2 = (\beta_iz_i)^2. \tag{10}$$

Taking the difference of any two of these equations yields

$$(\alpha_j - \alpha_i)q^2 = (\beta_i z_i - \beta_j z_j)(\beta_i z_i + \beta_j z_j).$$

Note that $\alpha_j - \alpha_i \in O_T^*$ while each of the two factors on the right is in O_T. It follows that each of these factors is made from primes $\pi | p$ in O_T. Further we may assume these factors are coprime, since if $\pi | p$ divides $2\beta_i z_i$ and $p > 2$ then from (10) π divides x.

Without loss of generality, we assume that there is a prime $\pi \in O_T$ dividing $\beta_1 z_1 + \beta_2 z_2$. If π does not divide $\beta_2 z_2 + \beta_3 z_3$ then π does not divide $\beta_1 z_1 - \beta_3 z_3$. So Siegel's identity

$$\frac{\beta_1 z_1 + \beta_2 z_2}{\beta_1 z_1 - \beta_3 z_3} - \frac{\beta_2 z_2 + \beta_3 z_3}{\beta_1 z_1 - \beta_3 z_3} = 1$$

gives

$$a_p^2 u + b_p^2 v = c_p^2 \tag{11}$$

where $a_p, b_p, c_p \in O_T$ divide q, are not all T-units and are pairwise coprime. If π divides $\beta_2 z_2 + \beta_3 z_3$ then π divides $\beta_1 z_1 - \beta_3 z_3$ so π does not divide $\beta_1 z_1 + \beta_3 z_3$. Then Siegel's identity

$$\frac{\beta_2 z_2 + \beta_1 z_1}{\beta_2 z_2 - \beta_3 z_3} - \frac{\beta_1 z_1 + \beta_3 z_3}{\beta_2 z_2 - \beta_3 z_3} = 1$$

gives (11).

Since $q = p^f$ is a prime power with $f > 1$, each of a_p and b_p is itself an f^{th} power. Finally, we note that the group $O_T^*/(O_T^*)^{2f}$ is finite so we fix once and for all a set of coset representatives. Then, by (11), each solution to (8) gives us a solution of an equation:

$$ux^{2f} + vy^{2f} = 1, \qquad x, y \in L,$$

with $2f \geq 4$, where u and v belong to this finite set of representatives, which depends only upon T and f. Since each such curve has genus $(2f-1)(f-1) \geq 3$, Faltings' Theorem [10] guarantees there are only finitely many solutions. Since we have only finitely many such equations, we are done. □

2. Proof of Theorem 0.2

Let E and E' be two elliptic curves, defined over $\mathbb{Q}$. An *isogeny* is a non-zero homomorphism

$$\sigma : E' \to E$$

taking the zero of E' to the zero of E. There is a dual isogeny $\sigma^* : E \to E'$ and the composite homomorphisms $\sigma\sigma^*$ and $\sigma^*\sigma$ are multiplication by d on E and E' respectively, for some integer d, which is said to be the *degree* of the isogeny. The curves E and E' are said to be d-*isogenous* if there is an isogeny of degree d between them.

Definition 2.1. For any point $P \in E(\mathbb{Q})$ let $S(P)$ denote the non-archimedean valuations v in $M_{\mathbb{Q}}$ for which $|x(P)|_v > 1$. The definition of $S(P)$ depends upon the Weierstrass equation so we assume this equation has been fixed.

Theorem 2.2. *Let E denote an elliptic curve which is defined over $\mathbb{Q}$ and let $G \subset E(\mathbb{Q})$ denote a subset contained in the image of a subset G' of rational points under a non-trivial isogeny. Then there are only finitely many $P \in G$ for which $S(P)$ consists of a single valuation: these points are effectively computable and they are at most $c^{(r_G+1)\omega(\Delta_E)}$ in number.*

Theorem 2.2 will be proved in Section 2.2 following a section with some basic properties of heights under isogeny.

2.1. **Heights.** Write

$$h_v(\alpha) = \log \max\{1, |\alpha|_v\}, \tag{12}$$

for the local (logarithmic) height at v. The naïve global logarithmic height of Q is defined to be

$$h(\alpha) = \sum_{v \in M_{\mathbb{Q}}} h_v(\alpha) = \sum_{v \in M_{\mathbb{Q}}} \log \max\{1, |\alpha|_v\},$$

the sum running over all the valuations of $\mathbb{Q}$. If P denotes any rational point on an elliptic curve, we write $h_v(P) = h_v(x(P))$ and $h(P) = h(x(P))$. Usually, in the literature, the global height is further normalized by dividing by 2.

Suppose P denotes a rational point of E. The theory of heights gives an estimate for

$$h(P) = \widehat{h}(P) + O(1),$$

where $\widehat{h}(P)$ denotes the canonical height of P. The canonical height enjoys the additional property that $\widehat{h}(mP) = m^2\widehat{h}(P)$ for any $m \in \mathbb{Z}$. More generally, if $\sigma : E' \to E$ denotes a d-isogeny then for $P' \in E'(\mathbb{Q})$

$$\widehat{h}(\sigma(P')) = d\widehat{h}(P'). \tag{13}$$

Lemma 2.3. *Suppose $P_1, \dots, P_r \in E(\mathbb{Q})$ are independent rational points and T is a torsion point. Then*

$$h_v(n_1P_1 + \cdots + n_rP_r + T) = O(\log |\underline{n}|(\log \log |\underline{n}|)^{r+2}),$$

for any valuation v where $|\underline{n}| = \max\{|n_1|, \dots, |n_r|\}$ for $\underline{n} \in \mathbb{Z}^r$. This can be written

$$\log |x(P)|_v = O(\log \widehat{h}(P)(\log\log \widehat{h}(P))^{r+2}), \tag{14}$$

for any $P \in E(\mathbb{Q})$.

Corollary 2.4. *With the same notation as Lemma 2.3, let S be any fixed, finite set of valuations of $\mathbb{Q}$. Then*

$$\sum_{v\in S} h_v(n_1P_1 + \cdots + n_rP_r + T) = O((\log |\underline{n}|)^2).$$

This can be written

$$\sum_{v\in S} h_v(P) = O((\log \widehat{h}(P))^2), \tag{15}$$

for any $P \in E(\mathbb{Q})$.

Proof of Lemma 2.3. We will detail a proof for the archimedean valuation only. The proof for non-archimedean valuations is similar. The estimate in Lemma 2.3 follows from an appropriate upper bound for $|x(n_1P_1 + \cdots + n_rP_r)|_v$. Putting the given model of the curve into a short Weierstrass equation only translates x by at most a constant. Let z_{P_i} correspond to P_i under an analytic isomorphism $E(\mathbb{C}) \simeq \mathbb{C}/L$, for some lattice L, with z_T corresponding to T. Thus we may assume that the x-coordinate of a point is given using the Weierstrass $\wp$-function with Laurent expansion in even powers of z,

$$x = \wp_L(z) = \frac{1}{z^2} + c_0 + c_2z^2 + \dots$$

Write $\{n_1z_{P_1} + \cdots + n_rz_{P_r} + z_T\}$ for $n_1z_{P_1} + \cdots + n_rz_{P_r} + z_T$ modulo L. When the quantity $|x(n_1P_1 + \cdots + n_rP_r + T)|$ is large it means $n_1P_1 + \cdots + n_rP_r + T$ is close to zero modulo L, thus the quantities $|x(n_1P_1 + \cdots + n_rP_r + T)|$ and $1/|\{n_1z_{P_1} + \cdots + n_rz_{P_r} + z_T\}|^2$ are commensurate. On the complex torus, this means the elliptic logarithm is close to zero. So it is sufficient to supply a lower bound for $|\{n_1z_{P_1} + \cdots + n_rz_{P_r} + z_T\}|$ and this can be given by elliptic transcendence theory (see [3]). We use Théorème 2.1 in [3] but see also [18] where an explicit version of David's Theorem appears on page 20. The nature of the bound is

$$\log |x(n_1P_1 + \cdots + n_rP_r + T)| \ll \log |\underline{n}|(\log\log |\underline{n}|)^{r+2}, \tag{16}$$

where the implied constant depends upon E, the valuation v and the points $P_1, \dots, P_r$.

For the final assertion, we need only note that the global canonical height $\hat{h}(n_1P_1 + \cdots + n_rP_r + T)$ is a positive definite quadratic form in $n_1, ..., n_r$, and hence comensurate with $|\underline{n}|^2$. □

We will need some more theory of elliptic curves over local fields, see [15]. For every non-archimedean valuation v, write ord_v for the corresponding order function. There is a subgroup of the group of $\mathbb{Q}_v$-rational points:

$$E_1(\mathbb{Q}_v) = \{O\} \cup \{P \in E(\mathbb{Q}_v) : \text{ord}_v(x(P)) \leq -2\}.$$

In [15], Silverman proves the following.

Proposition 2.5. *For all $P \in E_1(\mathbb{Q}_v)$ and all $d \in \mathbb{Z}$:*

$$\log|x(mP)|_v = \log|x(P)|_v - \log|m|_v. \tag{17}$$

For finitely many (bad) primes p, the reduction of E is not an elliptic curve because the reduced curve is singular. We write S_E for the set of valuations in $M_{\mathbb{Q}}$ corresponding to all such primes. The equation (17) then yields the following corollary:

Corollary 2.6. *Suppose $\sigma : E' \to E$ is a d-isogeny and $P' \in E_1'(\mathbb{Q}_v)$. If $v \notin S_E$ then $h_v(\sigma(P')) \geq h_v(P')$. The local heights are related by the formula*

$$h_v(\sigma(P')) = h_v(P') + O(1), \tag{18}$$

where the implied constant depends only upon the isogeny and is independent of P'.

Proof. Suppose v corresponds to the prime p. Provided $v \notin S_E$, both curves and the isogeny can be reduced modulo powers of p and the first statement in the Corollary follows. Applying the dual isogeny σ^* gives a similar inequality $h_v(\sigma^*(P)) \geq h_v(P)$, for all $P \in E_1(\mathbb{Q}_v)$. However, composing σ with its dual gives multiplication by d on E'. Now (17) applies to prove (18). □

2.2. **Proof of Theorem 2.2.**

Suppose G' is a subset of $E'(\mathbb{Q})$ and $\sigma : E' \to E$ is a d-isogeny with $\sigma(G') = G$. From (13),

$$\widehat{h}(P) = d\widehat{h}(P'), \tag{19}$$

where $\widehat{h}$ denotes the canonical heights of rational points on E and E'.

Suppose $S(P)$ consists of the single valuation v. If $v \in S_E$ then, by (15), we have

$$\widehat{h}(P') = O((\log \widehat{h}(P'))^2).$$

If $v \notin S_E$ then $P \in E_1(\mathbb{Q}_v)$ and, by reduction, $S(P') \subset S(P)$. Again by (15),

$$h(P) - h_v(P) = O((\log \widehat{h}(P'))^2) = h(P') - h_v(P'). \tag{20}$$

Now the canonical height differs from the naï̈ve height by a bounded amount so we are justified in using the canonical height in (20). It follows from (19) that

$$d\widehat{h}(P') - h_v(P) = O((\log \widehat{h}(P'))^2).$$

However, from (18)

$$h_v(P') - h_v(P) = O(1).$$

Subtracting these last two formulae, and dividing by $d-1 > 0$, gives

$$\widehat{h}(P') = O((\log \widehat{h}(P'))^2), \tag{21}$$

with an implied constant which is effectively computable. In particular, we have obtained the same inequality for any valuation v. Equation (21) bounds the height $\widehat{h}(P')$ so can only be satisfied by finitely many points P', which can be computed effectively.

Finally, we estimate the number of exceptional points, using a strong form of Siegel's Theorem, proved by Gross and Silverman. There is a non-trivial torsion point T' in the kernel of $\sigma : E' \to E$. Any isogeny factorizes as a product of isogenies of prime degree so, since the rank r_G and the discriminant Δ_E are preserved under isogeny, we may assume from now that σ has prime degree. Let K denote a number field over which T' is defined. By Mazur's famous result ([12, Theorem 1]), only finitely many primes can occur as degrees of prime degree isogenies which map onto rational points (the largest of which is 163). Let S denote the subset of $M_{\mathbb{Q}}$ consisting of all such prime degrees, together with the primes of bad reduction (in S_E). Let S_K denote the subset of M_K consisting of all places above those in S, together with the places dividing the denominator of T'.

Now the points P' and $P' + T'$ both map to P under σ. It follows that if P' (respectively $P' + T'$) has denominator divisible by a place of good reduction w (respectively w'), then w (respectively w') is guaranteed to appear in the denominator of P. Moreover, if $w, w' \notin S_K$, they are guaranteed to be distinct: indeed, any good reduction place dividing the denominator of both points will divide the denominator of T' and hence lie in S_K. Further, since P' is a $\mathbb{Q}$-rational point, w' is coprime to the prime of $\mathbb{Q}$ below w so there are two distinct primes of $\mathbb{Q}$ dividing B_P.

This ensures B_P cannot be a prime power unless either P' or $P'+T'$ is an S_K-integral point on E'. By the theorem of Gross and Silverman [11, Theorem 0.1], there are at most

$$d\eta^{r\delta(j_{E'})+|S_K|}$$

S_K-integral points in $E'(K)$, for an explicit constant η, where $d=[K:\mathbb{Q}]$ and $\delta(j_{E'})$ denotes the number of primes dividing the denominator of the j-invariant of E'. In their paper, r denotes the rank of the group $E(K)$; however, their results are valid for the number of S_K-integral points inside a subgroup of rank r. Since the primes dividing the denominator of $j_{E'}$ divide $\Delta_{E'}=\Delta_E$, since $|S_K|$ is a bounded multiple of $d\omega(\Delta_E)$, and since d is uniformly bounded by Mazur's Theorem, the bound in (4) follows. □

2.3. **Uniformity.** Under the assumption that G consists of a rank-1 subgroup of $E(\mathbb{Q})$, we may harness the ideas in Section 2.2 to explain how these might be used as part of a proof of uniformity where a descent is possible. In the rank-1 case, the inequality (21) can be stated more explicitly. Let P denote a generator of G and $\sigma(P')=P$. Writing $h'=\widehat{h}(P')$ and invoking the explicit form of David's Theorem in [18] shows that the integers n for which $S(nP)$ consists of a single valuation must satisfy

$$h'n^2<\tau\log n(\log\log n+\log\Delta_{E'})^3, \tag{22}$$

where τ denotes a uniform bound. Lang's Conjecture asserts a uniform upper bound for $(\log\Delta_{E'})/h'$. If the dependence upon $\log\Delta_{E'}$ on the right hand side of (22) were linear, then Lang's Conjecture would guarantee a uniform upper bound for the number of prime square denominators in the sequence $x(nP)$ when descent is possible.

The reason Example 0.3 works is that Lang's Conjecture can be proved in an explicit manner for 1-parameter families such as this [17]. Also, it is possible to obtain a stronger form of Lemma 2.3 without transcendence theory: since P lies off the connected component of the identity so do all its odd multiples and for these an upper bound for the x-coordinate exists. Also, (17) allows an easy treatment of the bad reduction primes by showing the local heights $h_v(nP)$ are each $O(\log n)$.

3. The curve $u^3+v^3=D$

In [7], it was proved that the integers B_P are prime powers for only finitely many $\mathbb{Q}$-points P. The proof used the well-known bi-rational equivalence of (5) with the curve

$$y^2=x^3-432D^2.$$

Example As Ramanujan famously pointed out, the taxi-cab equation

$$u^3 + v^3 = 1729, \tag{23}$$

has two distinct integral solutions. These give rise to points $P = [1, 12]$ and $Q = [9, 10]$ on the elliptic curve (23). The only rational points on (23) which seem to yield prime power denominators are $2Q$ and $P+Q$ (and their inverses).

Proof of Theorem 0.4. We assume that D is integral; if D is not integral then we can scale by a non-zero integer to reduce to this case. Firstly, we recall the easy proof of Siegel's Theorem for curves in homogeneous form (5). The equation factorizes as

$$(u + v)(u^2 - uv + v^2) = D$$

so

$$|u^2 - uv + v^2| \leq |D|.$$

But the left hand side of this is $(u - v/2)^2 + 3v^2/4$ so $|v|^2 \leq 4|D|/3$. Hence the result with an explicit bound for $|v|$. The bound for $|u|$ is identical.

This bounds the number of solutions as $O(|D|^{1/2})$ but we can easily improve on this. First we have $u + v = m$, and $u^2 - uv + v^2 = n$, for some integers m, n such that $mn = D$ and $\gcd(m, n)|3$. If ζ is a non-trivial cube root of unity, then we get

$$(u + \zeta v)(u - \zeta v) = n,$$

where the factors on the left hand side have greatest common divisor dividing 2. The number of ways of factorizing n in this way is $O(2^{2\omega(n)})$ so the total number of solution (u, v) is $O(\mu^{\omega(D)})$, for some (explicit) uniform constant μ.

Now suppose

$$(u + v)(u^2 - uv + v^2) = u^3 + v^3 = Dq^3$$

where $q = p^f$ is a prime power and u, v are integers coprime to q. We consider first the case $p > 3$. Then q cannot possess a factor in common with both brackets. Hence one bracket is m and the other is nq^3, where $mn = D$ and $\gcd(m, n)|3$. If the quadratic bracket is bounded then we bound the number of solutions as before, so we assume

$$u + v = m \text{ and } (u + \zeta v)(u - \zeta v) = nq^3.$$

Since $u + \zeta v$ and $u - \zeta v$ are coprime, we get

$$u + v = m \text{ and } u - \zeta v = k\rho^3$$

where k divides n and ρ divides q in $\mathbb{Z}[\zeta]$. If we write $k = c + d\zeta$ and $\rho = a + b\zeta$, with $a, b, c, d \in \mathbb{Z}$, then we can write u and v explicitly in terms of a, b, c, d. Substituting into the equation $u + v = m$, we get

$$(c+d)a^3 + (3c-6d)a^2b + (3d-6c)ab^2 + (c+d)b^3 = m.$$

For each of the finitely many values of c and d, this is a Thue Equation and it is non-singular – that is, for any non-zero c and d, the cubic

$$(c+d)X^3 + (3c-6d)X^2 + (3d-6c)X + (c+d)$$

does not have repeated roots, since its discriminant is

$$729c^4 - 1458dc^3 + 2187d^2c^2 - 1458d^3c + 729d^4 = 729(c^2 - cd + d^2)^2,$$

which does not vanish unless $c = d = 0$. Thus each of the finitely many Thue equations has finitely many solutions so there were only finitely many values of q.

By [9, Theorem 1] (see also *op. cit.* page 122), a non-singular integral cubic Thue Equation

$$F(x,y) = m,$$

with m cube-free, has a number of integral solutions which is bounded by $\mu^{\omega(m)}$, for some (explicit) uniform constant μ. This must be multiplied by the total number of equations, which depends only upon the number of factorizations of $mn = D$ with $\gcd(m,n)|3$, so does not change the shape of the bound claimed by the theorem.

Finally, the cases $p = 2, 3$ are dealt with similarly, with minor alterations. The point is that the greatest common divisors of the various brackets are uniformly bounded, so the shape of the final number of solutions is unchanged. □

References

[1] J. W. S. Cassels, *Lectures on Elliptic Curves,* London Mathematical Society Student Texts 24, Cambridge University Press, Cambridge, 1991.

[2] D. V. Chudnovsky and G. V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests,* Adv. in Appl. Math. 7 (1986), 385–434.

[3] S. David, *Minorations de formes linéaires de logarithmes elliptiques,* Mém. Soc. Math. France (N.S.) No. 62 (1995).

[4] M. Einsiedler, G. Everest and T. Ward, *Primes in elliptic divisibility sequences,* LMS J. Comp. Math. 4 (2001), 1–13.

[5] N. Elkies, *Nontorsion points of low height on elliptic curves over $\mathbb{Q}$,* `http://www.math.harvard.edu/~elkies/low_height.html`

[6] G. Everest, P. Rogers and T. Ward, *A higher rank Mersenne problem,* Algorithmic number theory (Sydney, 2002), 95–107, Lecture Notes in Comput. Sci. 2369, Springer, Berlin, 2002.

[7] G. Everest, V. Miller and N. Stephens, *Primes generated by elliptic curves,*. Proc. Amer. Math. Soc. 132 (2004), 955–963.

[8] G. Everest and H. King, *Prime powers in elliptic divisibility sequences.,* Math. Comp. 74 (2005), 2061–2071.

[9] J.-H. Evertse, *The number of solutions of the Thue-Mahler equation,* J. Reine Angew. Math. 482 (1997), 121–149.

[10] G. Faltings, *Endlichkeitsätze für abelschen Varietäten über Zahlkörper,* Invent. Math. 73 (1983), 349–366.

[11] R. Gross and J. Silverman, *S-integer points on elliptic curves,* Pacific J. Math. 167 (1995), 263–288.

[12] B. Mazur, *Rational isogenies of prime degree,* Invent. Math. 44 (1978), 129–169.

[13] J. Reynolds, *Rational Points on Elliptic Curves,* PhD Thesis, University of East Anglia, 2007.

[14] P. Rogers, *2-D Elliptic Divisibility Sequences,* `http://www.mth.uea.ac.uk/~h090/2deds.htm`

[15] J. H. Silverman, *The Arithmetic of Elliptic Curves,* Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986.

[16] J. H. Silverman, *A quantitative version of Siegel's Theorem: Integral points on elliptic curves and Catalan curves,* J. Reine Angew. Math. 378 (1987), 60–100.

[17] J. H. Silverman, *Variation of the canonical height on elliptic surfaces. I. Three examples,* J. Reine Angew. Math. 426 (1992), 151–178.

[18] R. J. Stroeker and N. Tzanakis, Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms, Acta. Arith. 67 (1994), 177–196.

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, UK.

E-mail address: `g.everest@uea.ac.uk`